Group Rings, G-Codes and Constructions of Self-Dual and Formally Self-Dual Codes

Steven T. Dougherty
Department of Mathematics
University of Scranton
Scranton, PA 18510
USA
Joseph Gildea
Rhian Taylor
University of Chester
Chester, UK
Alexander Tylyshchak
Department of Algebra
Uzhgorod State University
Ukraine

September 10, 2017

Abstract

We describe G-codes, which are codes that are ideals in a group ring, where the ring is a finite commutative Frobenius ring and G is an arbitrary finite group. We prove that the dual of a G-code is also a G-code. We give constructions of self-dual and formally self-dual codes in this setting and we improve the existing construction given in [13] by showing that one of the conditions given in the theorem is unnecessary and, moreover, it restricts the number of self-dual codes obtained by the construction. We show that several of the standard constructions of self-dual codes are found within our general framework. We prove that our constructed codes must have an automorphism group that contains G as a subgroup. We also prove that a common construction technique for producing self-dual codes cannot produce the putative $[72, 36, 16]$ Type II code. Additionally, we show precisely which groups can be used to construct the extremal

Type II codes over length 24 and 48. We define quasi-G codes and give a construction of these codes.

Key Words: Group rings; self-dual codes; codes over rings.

1 Introduction

Cyclic codes are characterized by the fact that the cyclic shift of any element in the code is an element in the code. These codes are one of the most widely studied families of codes. This is due, for the most part, to the fact that cyclic codes have an algebraic description as ideals in the polynomial ring $R[x]/\langle x^n - 1\rangle$ where R is a Frobenius ring and n is the length of the code. To classify cyclic codes, it is simply a matter of finding ideals in this ring via a factorization of $x^n - 1$ over R.

One of the key results about cyclic codes is that the dual code of a cyclic code is a cyclic code. This result allows for the complete study of cyclic codes to be done in the canonical algebraic setting. Cyclic codes have also been generalized in numerous ways, specifically to constacyclic and negacyclic codes where $x^n - 1$ is replaced with $x^n - \lambda$ for constacyclic codes and $x^n + 1$ for negacyclic codes (that is $\lambda = -1$).

An alternate view of cyclic codes is to see them as ideals in the group ring RC_n where C_n is the cyclic group of order n. In this paper, we will study codes as ideals in an arbitrary group ring RG. This allows for an algebraic description of these codes as well as ensuring that the codes have a given group in their automorphism group. For very early work in this direction, see two papers by F.J. MacWilliams, [15] and [16]. We shall refer to codes that are ideals in the group ring RG as G-codes. We shall prove here that, like cyclic codes, the dual of a G-code is again a G-code.

Quasi-cyclic codes are another generalization of cyclic codes. The codes have received less attention largely because they do not have a canonical representation in an algebraic setting. We make a generalization of this concept to quasi-G cyclic codes. We give a construction, like that in [6] for cyclic codes, for quasi-G cyclic codes.

Self-dual codes over fields and rings are one of the most important and widely studied families of codes. They have interesting connections to groups, designs, lattices and other objects as well. As such, constructions of interesting self-dual codes are an important area of study in coding theory. In [13], Hurley gave a construction of self-dual codes from elements in a group algebra. The constructions were done generally in the group algebra $\mathbb{F}_2 D_{2k}$, where D_{2k} is the dihedral group of order $2k$. In [18], McLoughlin gave a construction of the extremal $[48, 24, 12]$ using this construction technique. Additionally, numerous techniques have been described using commutative Frobenius rings to construct binary self-dual and formally self-dual codes by Yildiz, Karadeniz and others (see [9], [10], [11] for example).

In this paper, we expand this construction to codes over finite commutative Frobenius rings and show how to construct isodual and formally self-dual codes as well. Additionally, we construct self-dual and formally self-dual codes over various families of rings, which, in turn, give formally self-dual and self-dual binary codes via a Gray map. We consider additional groups as well and expand the constructions using these groups.

1.1 Codes

The alphabet that we shall use for our codes is a finite commutative ring. It is also possible to study codes over non-commutative rings as well but we shall restrict ourselves to commutative rings in this paper. As such, from this point on we assume that all rings are commutative. Since the MacWilliams relations, which are fundamental in coding theory, only hold over Frobenius rings, we restrict ourselves to finite commutative Frobenius rings. For a description of coding theory in this setting see [5].

We begin by giving a characterization of Frobenius rings. Let R be a finite ring. We assume that all rings contain a multiplicative identity. Let $\widehat{R}$ be the character module of the ring R. Then for a finite ring R the following are equivalent.

- R is a Frobenius ring.
- As a left module, $\widehat{R} \cong {}_R R$.
- As a right module, $\widehat{R} \cong R_R$.

For commutative rings we can say that the R-module R is injective and that if R is a finite local ring with maximal ideal $\mathfrak{m}$ and residue field $\mathbf{k}$, then a Frobenius ring has $\dim_{\mathbf{k}} \mathrm{Ann}(\mathfrak{m}) = 1$. All of the rings used as alphabets in this paper will be assumed to be finite, commutative and Frobenius.

A code over R of length n is a subset of R^n. If the code is a submodule of R^n, then we say that the code is a linear code. We attach to the ambient space the usual inner-product, namely $[\mathbf{v}, \mathbf{w}] = \sum v_i w_i$ and define the orthogonal with respect to this inner-product as

$$C^{\perp} = \{\mathbf{v} \in R^n \mid [\mathbf{v}, \mathbf{w}] = 0, \ \forall \mathbf{w} \in C\}.$$

There is a unique orthogonal code because the ring is commutative. In the non-commutative case, there is both a left and right orthogonal. A code is said to be self-orthogonal if $C \subseteq C^{\perp}$ and self-dual if $C = C^{\perp}$. We say that two codes C and C' are equivalent if C' can be formed from C by permuting the coordinates of C. In some works about codes over rings, multiplication of a coordinate by a unit is allowed when defining equivalence, but note that we only allow permutation of coordinates in our definition of equivalence. A code C is said to be isodual if C and $C^{\perp}$ are equivalent codes. The automorphism group of a code C,

denoted $Aut(G)$, consists of all permutations of the coordinates of the code that fix the code.

Let C be a code over a ring $R = \{a_0, a_1, \ldots, a_{r-1}\}$. The complete weight enumerator for the code C is defined as:

$$cwe_C(x_{a_0}, x_{a_1}, \ldots, x_{a_{r-1}}) = \sum_{\mathbf{c} \in C} \prod_{i=0}^{r-1} x_{a_i}^{n_i(\mathbf{c})} \tag{1}$$

where there are $n_i(\mathbf{c})$ occurrences of a_i in the vector $\mathbf{c}$.

The Hamming weight of a vector $\mathbf{v} \in R^n$ is $wt_H(\mathbf{v}) = |\{i \mid v_i \neq 0\}|$. The Hamming weight enumerator is given by

$$W_C(x, y) = \sum_{\mathbf{c} \in C} x^{n - wt_H(\mathbf{c})} y^{wt_H(\mathbf{c})} = cwe_C(x, y, y, \ldots, y). \tag{2}$$

We say that a code is formally self-dual with respect to some weight enumerator if the code and its orthogonal have the same weight enumerator. It is possible for a code to be formally self-dual with respect to one weight enumerator and not another. For example, many codes are formally self-dual with respect to the Hamming weight enumerator without being formally self-dual with respect to the complete weight enumerator. Note that a self-dual code is also necessarily formally self-dual with respect to all weight enumerators.

Other weight enumerators are also possible, such as the symmetric weight enumerator or the Lee weight enumerator (which will be defined later) for specific rings. Since we only allow permutation of coordinates in our definition of equivalence, we have that if C is isodual, then any weight enumerator for the code C (complete, Hamming, symmetric, etc.) is identical to the weight enumerator of its orthogonal. This implies the following lemma which we will use in our constructions.

Lemma 1.1. *If C is an isodual code then it is formally self-dual with respect to any weight enumerator.*

As mentioned before, we restrict ourselves to Frobenius rings since this is the class of rings for which MacWilliams relations exist. That is, the weight enumerator of a code over a Frobenius ring uniquely determines the weight enumerator of its orthogonal. See [5] for a complete description of these results. The MacWilliams relations imply that for a code C over a Frobenius ring R we have $|C||C^{\perp}| = |R|^n$. This often fails for codes over non-Frobenius rings. In that sense, it is very difficult to discuss self-dual and formally self-dual codes over non-Frobenius rings. Moreover, this provides an easy way to prove that a ring is not Frobenius, that is, simply find an ideal I whose annihilator does not have cardinality $|R|/|I|$.

A Gray map is a distance preserving map ϕ from R to $\mathbb{F}_2^t$ for some t. We define the Lee weight, $wt_L(a)$ of an element $a \in R$ as the Hamming weight of $\phi(a)$. We then extend this to

R^n by saying that the Lee weight of a vector is the sum of the Lee weights of the coordinates of the vector. Then the Lee weight enumerator of a code C over R with an associated Gray map is defined as:

$$L_C(x,y) = \sum_{\mathbf{c}\in C} x^{N-wt_L(\mathbf{c})} y^{wt_L(\mathbf{c})}, \tag{3}$$

where N is the length of the binary image of the code C under the Gray map. Note that the Lee weight enumerator of a code C is the Hamming weight enumerator of the code $\phi(C)$.

1.2 Group Rings

We shall consider codes that are ideals inside of a group ring, where the ring is the alphabet of the code. We continue by giving the necessary definitions for group rings. Let G be a finite group or order n, then the group ring RG consists of $\sum_{i=1}^{n} \alpha_i g_i$, $\alpha_i \in R$, $g_i \in G$.

Addition in the group ring is done by coordinate addition, namely

$$\sum_{i=1}^{n} \alpha_i g_i + \sum_{i=1}^{n} \beta_i g_i = \sum_{i=1}^{n} (\alpha_i + \beta_i) g_i.$$

The product of two elements in a group ring is given by

$$(\sum_{i=1}^{n} \alpha_i g_i)(\sum_{j=1}^{n} \beta_j g_j) = \sum_{i,j} \alpha_i \beta_j g_i g_j.$$

This gives that the coefficient of g_i in the product is $\sum_{g_i g_j = g_k} \alpha_i \beta_j$.

Group rings are defined for groups and rings of arbitrary cardinality but, in this paper, we shall only be concerned with finite rings and finite groups since our alphabet for codes is a finite ring and codes are defined for finite length which corresponds to the size of the group. If R is a field then the term group algebra is usually used in this case since the structure is an algebra as well. Throughout this paper we use e_G to refer to the identity element of any group G.

We denote the space of n by n matrices with coefficients in R by $M_n(R)$. Note that $M_n(R)$ is, in general, a non-commutative ring since multiplication of matrices is not commutative.

A matrix M, where the indices are given by the elements in $\mathbb{Z}_n$, is said to be circulant if $M_{i,j} = M_{1,j-i \pmod n}$, that is the matrix is formed by cycling the first row to the right. A matrix M, where the indices are given by the elements in $\mathbb{Z}_n$, is said to be reverse circulant if $M_{i,j} = M_{1,j+i \pmod n}$, that is the matrix is formed by cycling the first row to the left. It is immediately clear from the definition that a reverse circulant matrix is symmetric, that is, $M = M^T$.

2 Matrix Construction

In this section, we shall give a construction of codes in R^n from the group ring RG. This construction was first given for codes over fields by Hurley in [13]. Let R be a finite commutative Frobenius ring and let $G = \{g_1, g_2, \ldots, g_n\}$ be a group of order n. Let $v = \alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \cdots + \alpha_{g_n} g_n \in RG$. Define the matrix $\sigma(v) \in M_n(R)$ to be

$$\sigma(v) = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \alpha_{g_1^{-1}g_3} & \cdots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \alpha_{g_2^{-1}g_3} & \cdots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \alpha_{g_n^{-1}g_3} & \cdots & \alpha_{g_n^{-1}g_n} \end{pmatrix}. \tag{4}$$

The elements $g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}$ are simply the elements of the group G in some order. We take this as the ordering of the elements since it makes the constructions more natural.

For a given element $v \in RG$, we define the following code over the ring R:

$$C(v) = \langle \sigma(v) \rangle. \tag{5}$$

Namely, the code is formed by taking the row space of $\sigma(v)$ over the ring R. The code $C(v)$ is a linear code since it is the row space of a generator matrix, but it is not possible to determine the size of the code (or the dimension if R is a field) immediately from the matrix. In other words, the rows of the matrix $\sigma(v)$ are not necessarily linearly independent, although they may be, as we show in the following example.

Example 1. *Let R be a finite commutative Frobenius ring and let $G = \{g_1, g_2, \ldots, g_n\}$ be a group. Let $v_1 = \sum 0 g_i$. Then $\sigma(v_1)$ is the all zero matrix and $C(v_1) = \{\mathbf{0}\}$. Let $v_2 = \sum \alpha_i g_i$ with $\alpha_j = 1$ for some j and $\alpha_i = 0$ for $i \neq j$. Then $\sigma(v)$ is permutation equivalent to I_n, the n by n identity matrix, which gives that $C(v_2) = R^n$.*

We will say that two matrices are equivalent if they generate equivalent codes.

Example 2. *Let $v = (1+s+s^2+s^3)(1+t) \in \mathbb{F}_2 M_{16}$ where $M_{16} = \langle s, t \mid s^8 = t^2 = 1,\ st = ts^5 \rangle$ is the modular group of order 16. Then,*

$$\sigma(v) = \begin{pmatrix} 1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0 \\ 0&1&1&1&1&0&0&0&1&0&0&0&0&1&1&1 \\ 0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0 \\ 0&0&0&1&1&1&1&0&1&1&1&0&0&0&0&1 \\ 0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 1&0&0&0&0&1&1&1&0&1&1&1&1&0&0&0 \\ 1&1&0&0&0&0&1&1&1&1&0&0&0&0&1&1 \\ 1&1&1&0&0&0&0&1&0&0&0&1&1&1&1&0 \\ 1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0 \\ 1&0&0&0&0&1&1&1&0&1&1&1&1&0&0&0 \\ 0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0 \\ 1&1&1&0&0&0&0&1&0&0&0&1&1&1&1&0 \\ 0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0&1&1&1&1&0&0&0&1&0&0&0&0&1&1&1 \\ 1&1&0&0&0&0&1&1&1&1&0&0&0&0&1&1 \\ 0&0&0&1&1&1&1&0&1&1&1&0&0&0&0&1 \end{pmatrix}$$

and $\sigma(v)$ is equivalent to

$$\begin{pmatrix} 1&0&0&0&0&1&1&1&0&1&1&1&1&0&0&0 \\ 0&1&0&0&0&1&0&0&1&0&1&1&1&0&1&1 \\ 0&0&1&0&0&0&1&0&1&1&0&1&1&1&0&1 \\ 0&0&0&1&0&0&0&1&1&1&1&0&1&1&1&0 \\ 0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \end{pmatrix}.$$

Clearly, $C(v)$ is the $[16, 5, 8]$ Reed-Muller code.

We shall now show that the codes we construct are actually ideals in the group ring. We use this to get information about the automorphism group of the constructed code.

Theorem 2.1. *Let R be a finite commutative Frobenius ring and G a finite group of order n. Let $v \in RG$ and let $C(v)$ be the corresponding code in R^n. Let $I(v)$ be the set of elements of RG such that $\sum \alpha_i g_i \in I(v)$ if and only if $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in C(v)$. Then $I(v)$ is a left ideal in RG.*

Proof. The rows of $\sigma(v)$ consist precisely of the vectors that correspond to the elements hv in RG where h is any element of G. The sum of any two elements in $I(v)$ corresponds exactly to the sum of the corresponding elements in $C(v)$ and so $I(v)$ is closed under addition.

Let $w_1 = \sum \beta_i g_i \in RG$. Then if w_2 corresponds to a vector in $C(v)$, it is of the form $\sum \gamma_j h_j v$. Then $w_1 w_2 = \sum \beta_i g_i \sum \gamma_i h_i v = \sum \beta_i \gamma_j g_i h_j v$ which corresponds to an element in $C(v)$ and gives that the element is in $I(v)$. Therefore $I(v)$ is a left ideal of RG. □

Example 3. *Let $v = 1 + ba + ba^2 + ba^3 \in \mathbb{F}_2 D_8$ where $\langle a, b \rangle \cong D_8$. Then $\sigma(v) = \begin{pmatrix} 1&0&0&0&0&1&1&1 \\ 0&1&0&0&1&1&1&0 \\ 0&0&1&0&1&1&0&1 \\ 0&0&0&1&1&0&1&1 \\ 0&1&1&1&1&0&0&0 \\ 1&1&1&0&0&1&0&0 \\ 1&1&0&1&0&0&1&0 \\ 1&0&1&1&0&0&0&1 \end{pmatrix}$ and $\sigma(v)$ is equivalent to $A = \begin{pmatrix} 1&0&0&0&0&1&1&1 \\ 0&1&0&0&1&1&1&0 \\ 0&0&1&0&1&1&0&1 \\ 0&0&0&1&1&0&1&1 \end{pmatrix}$. Clearly $C(v) = \langle \sigma(v) \rangle$ is the $[8, 4, 4]$ extended Hamming code. Let $v_1 = 1 + ba + ba^2 + ba^3 \in \mathbb{F}_2 D_8$, $v_2 = 1 + b + ba + ba^2 \in \mathbb{F}_2 D_8$, $v_3 = 1 + b + ba + ba^3 \in \mathbb{F}_2 D_8$ and $v_4 = 1 + b + ba^2 + ba^3 \in \mathbb{F}_2 D_8$ where v_i are the group ring element corresponding to the rows of A. Let $I(v) = \left\{ \sum_{i=1}^{4} \alpha_i v_i | \alpha_i \in \mathbb{F}_2 \right\}$. Then $I(v)$ is a left ideal of $\mathbb{F}_2 D_8$ and in particular $I(v)$ is the left principle ideal of $\mathbb{F}_2 D_8$ generated by v.*

Corollary 2.2. *Let R be a finite commutative Frobenius ring and G a finite group of order n. Let $v \in RG$ and let $C(v)$ be the corresponding code in R^n. Then the automorphism group of $C(v)$ has a subgroup isomorphic to G.*

Proof. Since $I(v)$ is an ideal in RG we have that $I(v)$ is held invariant by the action of the elements of G. It follows immediately that the automorphism group of $C(v)$ contains G as a subgroup. □

We note that our construction gives a natural generalization of cyclic codes since cyclic codes are ideals in RC_n where C_n is the cyclic group of order n. Cyclic codes are held invariant by the cyclic shift whereas our codes are held invariant by the action of the group G on the coordinates. Moreover, this is the strength of our construction technique. Namely, we can construct a code whose automorphism group must contain a given group. In this sense, when the group used is G, we can refer to a code that is an ideal in RG as G-codes, where G is replaced by the name of the code when known. Therefore, classically we can say cyclic codes, but we can know say dihedral codes or dicyclic codes. When something applies

to any group we can still say G-codes. It is immediate that a code of length n can only be a G-code for some G if it has a subgroup of its automorphism group of order n.

Example 4. *Let C be the extremal $[48, 24, 12]$ Pless symmetry code. The automorphism group of this code is $PSL(2, 47)$. A computation in GAP [12] shows that the only subgroup of $PSL(2, 47)$ of order 48 is D_{48}. Hence the only possible construction of this code by our technique must have $G = D_{48}$. This construction is given by McLoughlin in [18]. This gives that the Pless symmetry code is, in fact, a dihedral code.*

Combining the results in [2], [3], [4], [20], [21] and [22], we have that the automorphism group of a putative $[72, 36, 16]$ code must have order 1,2, 3, 4, or 5. See [8] for details on the automorphism group and a detailed description of this putative code. Since it is impossible for a group of order 72 to satisfy these we have the following corollary.

Corollary 2.3. *The putative $[72, 36, 16]$ code cannot be of the form $C(v)$ for any $v \in \mathbb{F}_2 G$ for any group G.*

Proof. The result follows immediately from Corollary 2.2 and the previous discussion. □

Note that a code whose automorphism group is trivial cannot be constructed by this technique.

2.1 The Family of Rings R_k

In this subsection, we shall describe a family of rings which is useful in producing binary formally self-dual codes via their associated Gray maps.

Define the ring R_k as

$$R_k = \mathbb{F}_2[u_1, u_2, \ldots, u_k]/\langle {u_i}^2, u_i u_j - u_j u_i \rangle. \tag{6}$$

These rings are local rings of characteristic 2 with maximal ideal $\mathfrak{m} = \langle u_1, u_2, \ldots, u_k \rangle$. This maximal ideal is also necessarily the Jacobson radical of the ring, which can be characterized as the intersection of all maximal ideals. The socle, which is the sum of all minimal ideals, for the ring R_k is $Soc(R_k) = \langle u_1 u_2 \cdots u_k \rangle = \mathfrak{m}^{\perp}$. We have that $|R_k| = 2^{2^k}$. The rings R_k were described in [9], [10], and [11].

We can describe a Gray map for R_k. We define $\phi_1(a + bu_1) = (b, a + b)$, where ϕ maps R to $\mathbb{F}_2^2$. Then view $R[u_1, u_2, \ldots, u_s]$ as $R[u_1, u_2, \ldots, u_{s-1}][u_s]$ and define $\phi_s(a+bu_s) = (b, a+b)$. Then the map ϕ_k is map from R_k to $\mathbb{F}_2^{2^k}$.

The following theorem appears in [11].

Theorem 2.4. *Let C be a self-dual code over R_k, then $\phi_k(C)$ is a self-dual code in $\mathbb{F}_2^{2^k}$.*

We shall give several examples where we construct self-dual codes over R_k using the method in the paper and then use the Gray map to construct a binary self-dual code of longer length.

2.2 Codes, Ideals and Orthogonals

One of the fundamental results about cyclic codes is that the orthogonal of a cyclic code is again a cyclic code. In this subsection, we generalize this results to codes that are ideals in a group ring. That is we show that if C is a G-code for some G then its orthogonal $C^{\perp}$ is also a G-code.

Let I be an ideal in a group ring RG. Define $\mathcal{R}(C) = \{w \mid vw = 0, \forall v \in I\}$. It is immediate that $\mathcal{R}(I)$ is an ideal of RG.

Let $v = a_{g_1}g_1 + a_{g_2}g_2 + \ldots a_{g_n}g_n \in RG$ and $C(v)$ be the corresponding code. Let $\Psi : RG \to R^n$ be the canonical map that sends $a_{g_1}g_1 + a_{g_2}g_2 + \ldots a_{g_n}g_n$ to $(a_{g_1}, a_{g_2}, \ldots, a_{g_n})$. Let I be the ideal $\Psi^{-1}(C)$. Let $\mathbf{w} = (w_1, w_2, \ldots, w_n) \in C^{\perp}$. Then

$$[(a_{g_j^{-1}g_1}, a_{g_j^{-1}g_2}, \ldots, a_{g_j^{-1}g_n}), (w_1, w_2, \ldots, w_n)] = 0, \forall j. \tag{7}$$

This gives that

$$\sum_{i=1}^{n} a_{g_j^{-1}g_i} w_i = 0, \ \forall j. \tag{8}$$

Let $w = \Psi^{-1}(\mathbf{w}) = \sum w_{g_i} g_i$ and define $\overline{\mathbf{w}} \in RG$ to be $\overline{\mathbf{w}} = b_{g_1}g_1 + b_{g_2}g_2 + \cdots + b_{g_n}g_n$ where

$$b_{g_i} = w_{g_i^{-1}}. \tag{9}$$

Then

$$\sum_{i=1}^{n} a_{g_j^{-1}g_i} w_i = 0 \implies \sum_{i=1}^{n} a_{g_j^{-1}g_i} b_{g_i^{-1}} = 0. \tag{10}$$

Then $g_j^{-1} g_i g_i^{-1} = g_j^{-1}$, hence this is the coefficient of g_j^{-1} in the product of $\overline{\mathbf{w}}$ and $g_j^{-1}v$. This gives that $\overline{\mathbf{w}} \in \mathcal{R}(I)$ if and only if $\mathbf{w} \in C^{\perp}$.

Let $\phi : R^n \to RG$ by $\phi(\mathbf{w}) = \overline{\mathbf{w}}$. It is clear that ϕ is a bijection between $C^{\perp}$ and $\mathcal{R}(\Psi^{-1}(C))$.

Theorem 2.5. *Let $C = C(v)$ be a code in RG formed from the vector $v \in RG$. Then $\Psi^{-1}(C^{\perp})$ is an ideal of RG.*

Proof. We have that $\Psi(\phi(C^{\perp}))$ is permutation equivalent to $C^{\perp}$ and $\phi(C^{\perp})$ is an ideal and so $\Psi^{-1}(C)$ is an ideal as well. □

This is a generalization of the well known result that the dual of a cyclic code is a cyclic code. The action induces by $\overline{\mathbf{w}}$ is the similar to the polynomial $\overline{f(x)}$ used in cyclic codes to generate the ideal in $R[x]/\langle x^n - 1\rangle$ corresponding to the dual code.

We can now generalize another important technique used in the theory of cyclic codes. Let R be a finite commutative Frobenius ring that is isomorphic via the Chinese Remainder Theorem to $R_1 \times R_2 \times \ldots R_s$. Let $CRT : R_1 \times R_2 \times \ldots R_s \to R$ be the map induced my the Chinese Remainder Theorem. See [5] for a complete description of the use of this map in coding theory.

Theorem 2.6. *Let C_i be a G-code over the ring R_i, that is C_i is an ideal in R_iG. Then $CRT(C_1, C_2, \ldots, C_s)$ is a G-code over R.*

Proof. Let $g \in G$ and $\mathbf{v}_i \in C_i$. Then $g\mathbf{v}_i \in C_i$ for all i. Then if $\mathbf{v} = CRT(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s)$ then $g\mathbf{v} = CRT(g\mathbf{v}_1, g\mathbf{v}_2, \ldots, g\mathbf{v}_s)$ and so $g\mathbf{v} \in C$ giving that C is an ideal in RG. □

It is well known that any Frobenius ring is isomorphic to the direct product under the Chinese Remainder Theorem of Frobenius local rings. Additionally, a principal ideal ring isomorphic to the direct product under the Chinese Remainder Theorem of chain rings. Therefore, to study G-codes what is really necessary is to study G-codes over local rings, of which, chain rings are a special family.

2.3 Self-Orthogonal Codes

The following is a rephrasing, in more general terms, of Theorem 1 in [13]. Specifically, in [13], R is assumed to be a field. The proof is identical and simply consists of showing that addition and multiplication is preserved.

Theorem 2.7. *Let R be a finite commutative Frobenius ring and let G be a group of order n. Then the map $\sigma : RG \to M_n(R)$ is an injective ring homomorphism.*

For an element $v = \sum \alpha_i g_i \in RG$, define the element $v^T \in RG$ as $v^T = \sum \alpha_i g_i^{-1}$. This is sometimes known as the canonical involution for the group ring. The reason this notation is used in this setting will be apparent by the next lemma.

The following is a straightforward generalization of a result in [13].

Lemma 2.8. *Let R be a finite commutative Frobenius ring and let G be a group of order n. For an element $v \in RG$, we have that $\sigma(v)^T = \sigma(v^T)$.*

Proof. The ij-th element of $\sigma(v^T)$ is $\alpha_{(g_i^{-1}g_j)^{-1}} = \alpha_{g_j^{-1}g_i}$ which is the ji-th element of $\sigma(v)$. □

We next give our first result about the structure of our constructed codes.

Lemma 2.9. *Let R be a finite commutative Frobenius ring and let G be a group of order n. If $v = v^T$ and $v^2 = 0$ then C_v is a self-orthogonal code.*

Proof. If $v = v^T$ then $\sigma(v)^T = \sigma(v^T)$ by Lemma 2.8. Then we have that $(\sigma(v)\sigma(v))_{ij}$ is the inner-product of the i-th and j-th rows of $\sigma(v)$. Since $v^2 = 0$, by Theorem 2.7 we have that $\sigma(v)\sigma(v) = \mathbf{0}$. This gives that any two rows of $\sigma(v)$ are orthogonal and hence they generate a self-orthogonal code. □

We can now use this lemma to construct self-dual codes. For codes over fields we could simply use the dimension of $\sigma(v)$, however over an arbitrary Frobenius ring we cannot determine the size of the generated code simply from the rank of the matrix. Therefore, we have the following theorem.

Theorem 2.10. *Let R be a finite commutative Frobenius ring and G be a group of order n, with v an element in RG. If $v = v^T$, $v^2 = 0$ and $|C_v| = |R|^{\frac{n}{2}}$ then C_v is a self-dual code.*

Proof. By Lemma 2.9 the code C_v is self-orthogonal and since $|C_v| = |R|^{\frac{n}{2}}$ we have that C_v is self-dual. □

Notice that unlike the field case we are not assuming that n is even. For example, let $R = R_k$ and G be the trivial group of size 1 with $v = u_i e_G$ where e_G is the identity of the group. Then $\sigma(v) = (u_i)$ and C_v is a self-dual code of length 1.

In the following example, we show the strength of this construction by constructing a code over R_1 using the alternating group on 4 letters which has an image under the associated Gray map of the length 24 extended Golay code.

Example 5. *We shall use the previous results to construct the binary Golay code from the ring R_1. Let $v = u(b + ab + ac + bc^2) + (bc + bc^2) + (1 + u)(c^2 + abc^2) \in R_1A_4$. Then, C_v is a self-dual code of length 12 over R_1. Hence $\phi_k(C)$ is a binary self-dual code of length 12 by Theorem 2.4. The binary code $\phi_k(C)$ has a generator matrix of the following form:* $\begin{pmatrix} I_{12} & A \end{pmatrix}$ *where* $A = \begin{pmatrix} 1&0&1&1&0&0&1&0&1&1&0&1 \\ 1&1&1&0&0&1&1&0&1&0&1&0 \\ 1&1&1&1&1&0&0&0&0&1&1&0 \\ 1&0&1&0&1&0&0&1&1&0&1&1 \\ 1&0&0&1&1&1&1&0&0&0&1&1 \\ 1&1&0&0&1&1&0&0&1&1&0&1 \\ 1&1&0&1&0&1&1&1&0&1&0&0 \\ 0&1&1&0&1&0&1&1&1&1&0&0 \\ 0&1&0&1&1&1&0&1&1&0&1&0 \\ 0&0&1&1&1&1&0&1&0&1&0&1 \\ 0&1&1&1&0&0&1&1&0&0&1&1 \\ 0&0&0&0&0&1&1&1&1&1&1&1 \end{pmatrix}$. *It is a simple computation to see that $\phi_k(C_v)$ is the $[24, 12, 8]$ Golay code.*

Lemma 2.11. *Let R be a finite commutative Frobenius ring and let G be a group of order n. If $v = \sum \alpha_i g_i$ and $w = \alpha_i g_i h$ for some $h \in G$ then C_v and C_w are equivalent codes.*

Proof. The generator matrix for C_w is formed from the generator matrix of C_v by permuting the columns corresponding to multiplication of the elements of G by h. Hence, the codes are equivalent. □

Example 6. *Let $v_1 = 1+xz+yz+xyz \in \mathbb{F}_2(C_2\times C_2\times C_2)$ where $\langle x, y, z\rangle \cong C_2\times C_2\times C_2$. Now $\sigma(v_1)$ is equivalent to $\begin{pmatrix} 1&0&0&0&0&1&1&1 \\ 0&1&0&0&1&0&1&1 \\ 0&0&1&0&1&1&0&1 \\ 0&0&0&1&1&1&1&0 \end{pmatrix}$. The code $C(v_1)$ is the the $[8, 4, 4]$ extended Hamming code. Next, let us consider $v_2 = (1+xz+yz+xyz)y = y+xz+z+xyz \in \mathbb{F}_2(C_2 \times C_2 \times C_2)$. Then $\sigma(v_2)$ is equivalent to $\begin{pmatrix} 1&0&0&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1 \\ 0&0&1&1&0&1&1&0 \\ 0&0&0&0&1&1&1&1 \end{pmatrix}$. Clearly $C(v_1)$ is equivalent to $C(v_2)$.*

3 Binary Golay Code

The self-dual binary Golay code is one of the most interesting codes. It has interesting connections to the Leech lattice and is an extension of the length 23 perfect Golay code. We

shall now consider constructions of the $[24, 12, 8]$ binary Golay code from $\mathbb{F}_2 G$ for various groups G.

It is well known that the automorphism group of the $[24, 12, 8]$ code is the Mathieu group M_{24}. Therefore, the only possible groups that can work for our construction are

$$SL(2,3),\ S_4,\ D_{24},\ (C_6 \times C_2) \rtimes C_2, C_3 \times D_8, C_2 \times A_4 \text{ and } C_2^2 \times D_6.^1$$

Initially, it was shown in [1] that the $[24, 12, 8]$ could be constructed from ideals in the group algebra $\mathbb{F}_2 S_4$ where S_4 is the symmetric group on 4 elements. See also [17] for similar results. In [19], the $[24, 12, 8]$ code was constructed from $\mathbb{F}_2 D_{24}$. We shall now separately consider the remaining cases.

3.1 The Group $C_3 \times D_8$

We begin by considering the group $C_3 \times D_8$. Let v be the element

$$v = \sum_{i=1}^{4} [a^{i-1}(\alpha_i + \alpha_{i+4} z + \alpha_{i+8} z^2) + b a^{i-1}(\alpha_{i+12} + \alpha_{i+16} z + \alpha_{i+20} z^2)] \in \mathbb{F}_2(C_3 \times D_8)$$

where $\langle z \rangle = C_3$, $\langle a, b \rangle = D_8$ and $\alpha_i \in \mathbb{F}_2$. Now

$$\sigma(v) = \begin{pmatrix} A & B \\ B & A \end{pmatrix}$$

$$\text{where } A = \begin{pmatrix} A_1 & A_2 & A_3 \\ A_3 & A_1 & A_2 \\ A_2 & A_3 & A_1 \end{pmatrix}, B = \begin{pmatrix} B_1 & B_2 & B_3 \\ B_3 & B_1 & B_2 \\ B_2 & B_3 & B_1 \end{pmatrix},$$

$$\begin{aligned} A_1 &= cir(\alpha_1, \alpha_2, \alpha_3, \alpha_4), \\ A_2 &= cir(\alpha_5, \alpha_6, \alpha_7, \alpha_8), \\ A_3 &= cir(\alpha_9, \alpha_{10}, \alpha_{11}, \alpha_{12}), \\ B_1 &= rcir(\alpha_{13}, \alpha_{14}, \alpha_{15}, \alpha_{16}), \\ B_2 &= rcir(\alpha_{17}, \alpha_{18}, \alpha_{19}, \alpha_{20}), \\ B_3 &= rcir(\alpha_{21}, \alpha_{22}, \alpha_{23}, \alpha_{24}) \end{aligned}$$

and $cir(\alpha_1, \alpha_2, \ldots, \alpha_n)$, $rcir(\alpha_1, \alpha_2, \ldots, \alpha_n)$ are circulant and reverse circulant matrices respectively and $\alpha_1, \alpha_2, \ldots, \alpha_n$ is the first row of the respective matrices. Clearly $\langle \sigma(v) \rangle$ is self-dual if $\sigma(v)^T = \sigma(v)$. Now, $\sigma(v)^T = \sigma(v)$ if and only if $a_2 = a_4$, $a_5 = a_9$, $a_6 = a_{12}$,

[1] These groups are SmallGroup(24,i) for $i \in \{3, 6, 8, 10, 12, 13, 14\}$ according to the GAP system [12].

$a_7 = a_{11}$, $a_8 = a_{10}$, $a_{17} = a_{21}$, $a_{18} = a_{22}$, $a_{19} = a_{23}$ and $a_{20} = a_{24}$. Next, consider elements of $\mathbb{F}_2(C_3 \times D_8)$ of the form

$$\{\alpha_1 + \alpha_2(a + a^3) + \alpha_3 a^2 + \alpha_4(z + z^2) + \alpha_5 az(1 + a^2 z) + \alpha_6 a^2 z(1 + z) + \alpha_7 az(a^2 + z) + \sum_{i=1}^{4} b(\alpha_{i+7} + \alpha_{i+11}(z + z^2))a^{i-1} \mid \alpha_i \in \mathbb{F}_2 \}$$

and in particular the element $v_1 = 1 + b[(\hat{a}+1) + (1+a)(\hat{z}+1)]$ of this set where $\hat{a} = \sum_{i=0}^{3} a^i$ and $\hat{z} = \sum_{i=0}^{2} z^i$. The matrix $\sigma(v_1)$ is equivalent to

$$\begin{pmatrix} I & A \\ A & I \end{pmatrix}$$

where

$$A = \begin{pmatrix} 0&1&1&1&1&1&0&0&1&1&0&0 \\ 1&1&1&0&1&0&0&1&1&0&0&1 \\ 1&1&0&1&0&0&1&1&0&0&1&1 \\ 1&0&1&1&0&1&1&0&0&1&1&0 \\ 1&1&0&0&0&1&1&1&1&1&0&0 \\ 1&0&0&1&1&1&1&0&1&0&0&1 \\ 0&0&1&1&1&1&0&1&0&0&1&1 \\ 0&1&1&0&1&0&1&1&0&1&1&0 \\ 1&1&0&0&1&1&0&0&0&1&1&1 \\ 1&0&0&1&1&0&0&1&1&1&1&0 \\ 0&0&1&1&0&0&1&1&1&1&0&1 \\ 0&1&1&0&0&1&1&0&1&0&1&1 \end{pmatrix}.$$

It is a small computation to see that $C(v_1)$ is the $[24, 12, 8]$ code. Moreover, it can be shown that the above set contains 128 elements that generate the $[24, 12, 8]$ code.

3.2 The Group $C_2 \times A_4$

Next we consider the group $C_2 \times A_4$. Let v be the element

$$v = \sum_{i=1}^{3}(\alpha_{4i-3} + \alpha_{4i-2}a + \alpha_{4i-1}b + \alpha_{4i}ab + \alpha_{4i+9}x + \alpha_{4i+10}xa + \alpha_{4i+11}xb + \alpha_{4i+21}xab)c^{i-1} \in \mathbb{F}_2(C_2 \times A_4)$$

where $\langle x \rangle = C_2$, $a = (1,2)(3,4)$, $b = (1,3)(2,4)$ and $c = (1,2,3)$ and $\alpha_i \in \mathbb{F}_2$. Now

$$\sigma(v) = \begin{pmatrix} A & B \\ B & A \end{pmatrix}$$

where $A = \begin{pmatrix} A_2 & A_2 & A_3 \\ A_4 & A_5 & A_6 \\ A_7 & A_8 & A_9 \end{pmatrix}$, $B = \begin{pmatrix} B_2 & B_2 & B_3 \\ B_4 & B_5 & B_6 \\ B_7 & B_8 & B_9 \end{pmatrix}$,

$A_1 = bc(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, $A_2 = bc(\alpha_5, \alpha_6, \alpha_7, \alpha_8)$, $A_3 = bc(\alpha_9, \alpha_{10}, \alpha_{11}, \alpha_{12})$,
$A_4 = bc(\alpha_9, \alpha_{12}, \alpha_{10}, \alpha_{11})$, $A_5 = bc(\alpha_1, \alpha_4, \alpha_2, \alpha_3)$, $A_6 = bc(\alpha_5, \alpha_8, \alpha_6, \alpha_7)$,
$A_7 = bc(\alpha_5, \alpha_7, \alpha_8, \alpha_6)$, $A_8 = bc(\alpha_9, \alpha_{11}, \alpha_{12}, \alpha_{10})$, $A_9 = bc(\alpha_1, \alpha_3, \alpha_4, \alpha_2)$,

$B_1 = bc(\alpha_{13}, \alpha_{14}, \alpha_{15}, \alpha_{16})$, $B_2 = bc(\alpha_{17}, \alpha_{18}, \alpha_{19}, \alpha_{20})$, $B_3 = bc(\alpha_{21}, \alpha_{22}, \alpha_{23}, \alpha_{24})$,
$B_4 = bc(\alpha_{21}, \alpha_{24}, \alpha_{22}, \alpha_{23})$, $B_5 = bc(\alpha_{13}, \alpha_{16}, \alpha_{14}, \alpha_{15})$, $B_6 = bc(\alpha_{17}, \alpha_{20}, \alpha_{18}, \alpha_{19})$,
$B_7 = bc(\alpha_{17}, \alpha_{19}, \alpha_{20}, \alpha_{18})$, $B_8 = bc(\alpha_{21}, \alpha_{23}, \alpha_{24}, \alpha_{22})$ and $B_9 = bc(\alpha_{13}, \alpha_{15}, \alpha_{16}, \alpha_{14})$
where $bc(a, b, c, d)$ is a matrix that takes the form $\begin{pmatrix} a & b & c & d \\ b & a & d & c \\ c & d & a & b \\ d & c & b & a \end{pmatrix}$. Now, $\sigma(v) = \sigma(v)^T$ if and only if $a_5 = a_9$, $a_6 = a_{12}$, $a_7 = a_{10}$, $a_8 = a_{11}$, $a_{17} = a_{21}$, $a_{18} = a_{24}$, $a_{19} = a_{24}$ and $a_{20} = a_{23}$. Next, consider elements of $\mathbb{F}_2(C_2 \times A_4)$ of the form

$$\{\sum_{i=0}^{1} x^i((\alpha_{8i+1} + \alpha_{8i+2}a + \alpha_{8i+3}b + \alpha_{8i+4}ab) + (\alpha_{8i+5} + \alpha_{8i+6}a + \alpha_{8i+7}b + \alpha_{8i+8}ab)(c + c^2)) \mid \alpha_i \in \mathbb{F}_2\},$$

and in particular the element $v_1 = 1 + x(1 + b(1 + a)(1 + c^2)) + xa(1 + b)c$ of this set. The matrix $\sigma(v_1)$ is equivalent to

$$\begin{pmatrix} I & A \\ A & I \end{pmatrix}$$

where

$$A = \begin{pmatrix} 1&0&1&1&0&1&0&1&0&0&1&1 \\ 0&1&1&1&1&0&1&0&0&0&1&1 \\ 1&1&1&0&0&1&0&1&1&1&0&0 \\ 1&1&0&1&1&0&1&0&1&1&0&0 \\ 0&1&0&1&1&1&0&1&0&1&1&0 \\ 1&0&1&0&1&1&1&0&1&0&0&1 \\ 0&1&0&1&0&1&1&1&1&0&0&1 \\ 1&0&1&0&1&0&1&1&0&1&1&0 \\ 0&0&1&1&0&1&1&0&1&1&1&0 \\ 0&0&1&1&1&0&0&1&1&1&0&1 \\ 1&1&0&0&1&0&0&1&1&0&1&1 \\ 1&1&0&0&0&1&1&0&0&1&1&1 \end{pmatrix}.$$

It is a small computation to see that $C(v_1)$ is the $[24, 12, 8]$ code. Moreover, it can be shown that the above set contains 384 elements that generate the $[24, 12, 8]$ code.

3.3 The Group $G = (C_6 \times C_2) \rtimes C_2$

Next we consider the group $G = (C_6 \times C_2) \rtimes C_2$. Let v be the element

$$v = \sum_{i=1}^{4}(\alpha_i y^{i-1} + \alpha_{i+4}xy^{i-1} + \alpha_{i+8}x^2y^{i-1} + \alpha_{i+12}y^{i-1}z + \alpha_{i+16}xy^{i-1}z + \alpha_{i+20}x^2y^{i-1}z)$$
$$\in \mathbb{F}_2((C_6 \times C_2) \rtimes C_2)$$

where $(C_6 \times C_2) \rtimes C_2 = \langle x, y, z \,|\, x^3 = y^4 = z^2 = 1,\, xy = yx^2,\, xz = zx,\, yz = zy^3 \rangle$ and $\alpha_i \in \mathbb{F}_2$. Now,

$$\sigma(v) = \begin{pmatrix}
\alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 & \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_{13} & \alpha_{14} & \alpha_{15} & \alpha_{16} & \alpha_{17} & \alpha_{18} & \alpha_{19} & \alpha_{20} & \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{24} \\
\alpha_2 & \alpha_1 & \alpha_{13} & \alpha_{10} & \alpha_{14} & \alpha_{12} & \alpha_9 & \alpha_{18} & \alpha_7 & \alpha_4 & \alpha_{24} & \alpha_6 & \alpha_3 & \alpha_5 & \alpha_{17} & \alpha_{22} & \alpha_{15} & \alpha_8 & \alpha_{21} & \alpha_{23} & \alpha_{19} & \alpha_{16} & \alpha_{20} & \alpha_{11} \\
\alpha_3 & \alpha_{13} & \alpha_1 & \alpha_{14} & \alpha_{10} & \alpha_{16} & \alpha_{17} & \alpha_{23} & \alpha_{15} & \alpha_5 & \alpha_{21} & \alpha_{22} & \alpha_2 & \alpha_4 & \alpha_9 & \alpha_6 & \alpha_7 & \alpha_{20} & \alpha_{24} & \alpha_{18} & \alpha_{11} & \alpha_{12} & \alpha_8 & \alpha_{19} \\
\alpha_{14} & \alpha_{10} & \alpha_4 & \alpha_1 & \alpha_2 & \alpha_7 & \alpha_{16} & \alpha_{24} & \alpha_{12} & \alpha_{13} & \alpha_{18} & \alpha_{15} & \alpha_5 & \alpha_3 & \alpha_{22} & \alpha_{17} & \alpha_6 & \alpha_{21} & \alpha_8 & \alpha_{11} & \alpha_{20} & \alpha_9 & \alpha_{19} & \alpha_{23} \\
\alpha_5 & \alpha_4 & \alpha_{10} & \alpha_2 & \alpha_1 & \alpha_9 & \alpha_{22} & \alpha_{11} & \alpha_6 & \alpha_3 & \alpha_8 & \alpha_{17} & \alpha_{14} & \alpha_{13} & \alpha_{16} & \alpha_{15} & \alpha_{12} & \alpha_{19} & \alpha_{18} & \alpha_{24} & \alpha_{23} & \alpha_7 & \alpha_{21} & \alpha_{20} \\
\alpha_{24} & \alpha_{11} & \alpha_{19} & \alpha_{17} & \alpha_9 & \alpha_1 & \alpha_8 & \alpha_4 & \alpha_{18} & \alpha_{15} & \alpha_{22} & \alpha_2 & \alpha_{21} & \alpha_7 & \alpha_{20} & \alpha_3 & \alpha_{23} & \alpha_{10} & \alpha_6 & \alpha_5 & \alpha_{12} & \alpha_{13} & \alpha_{14} & \alpha_{16} \\
\alpha_{17} & \alpha_9 & \alpha_7 & \alpha_{19} & \alpha_{21} & \alpha_{23} & \alpha_1 & \alpha_6 & \alpha_{13} & \alpha_{11} & \alpha_5 & \alpha_{18} & \alpha_{15} & \alpha_{24} & \alpha_2 & \alpha_8 & \alpha_3 & \alpha_{22} & \alpha_{14} & \alpha_{12} & \alpha_{10} & \alpha_{20} & \alpha_{16} & \alpha_4 \\
\alpha_{23} & \alpha_{18} & \alpha_8 & \alpha_6 & \alpha_{12} & \alpha_{14} & \alpha_{24} & \alpha_1 & \alpha_{21} & \alpha_{22} & \alpha_9 & \alpha_{10} & \alpha_{20} & \alpha_{16} & \alpha_{11} & \alpha_4 & \alpha_{19} & \alpha_{13} & \alpha_7 & \alpha_2 & \alpha_{15} & \alpha_5 & \alpha_3 & \alpha_{17} \\
\alpha_9 & \alpha_{17} & \alpha_{15} & \alpha_{11} & \alpha_{24} & \alpha_{18} & \alpha_{13} & \alpha_{22} & \alpha_1 & \alpha_{19} & \alpha_4 & \alpha_{23} & \alpha_7 & \alpha_{21} & \alpha_3 & \alpha_{20} & \alpha_2 & \alpha_6 & \alpha_{10} & \alpha_{16} & \alpha_{14} & \alpha_8 & \alpha_{12} & \alpha_5 \\
\alpha_{10} & \alpha_{14} & \alpha_5 & \alpha_{13} & \alpha_3 & \alpha_{15} & \alpha_{12} & \alpha_{21} & \alpha_{16} & \alpha_1 & \alpha_{23} & \alpha_7 & \alpha_4 & \alpha_2 & \alpha_6 & \alpha_9 & \alpha_{22} & \alpha_{24} & \alpha_{20} & \alpha_{19} & \alpha_8 & \alpha_{17} & \alpha_{11} & \alpha_{18} \\
\alpha_{12} & \alpha_6 & \alpha_{22} & \alpha_{18} & \alpha_{23} & \alpha_{21} & \alpha_5 & \alpha_9 & \alpha_{14} & \alpha_8 & \alpha_1 & \alpha_{19} & \alpha_{16} & \alpha_{20} & \alpha_4 & \alpha_{11} & \alpha_{10} & \alpha_7 & \alpha_{13} & \alpha_{17} & \alpha_3 & \alpha_{24} & \alpha_{15} & \alpha_2 \\
\alpha_{11} & \alpha_{24} & \alpha_{21} & \alpha_{15} & \alpha_7 & \alpha_2 & \alpha_{18} & \alpha_{10} & \alpha_8 & \alpha_{17} & \alpha_{16} & \alpha_1 & \alpha_{19} & \alpha_9 & \alpha_{23} & \alpha_{13} & \alpha_{20} & \alpha_4 & \alpha_{12} & \alpha_{14} & \alpha_6 & \alpha_3 & \alpha_5 & \alpha_{22} \\
\alpha_{13} & \alpha_3 & \alpha_2 & \alpha_5 & \alpha_4 & \alpha_{22} & \alpha_{15} & \alpha_{20} & \alpha_{17} & \alpha_{14} & \alpha_{19} & \alpha_{16} & \alpha_1 & \alpha_{10} & \alpha_7 & \alpha_{12} & \alpha_9 & \alpha_{23} & \alpha_{11} & \alpha_8 & \alpha_{24} & \alpha_6 & \alpha_{18} & \alpha_{21} \\
\alpha_4 & \alpha_5 & \alpha_{14} & \alpha_3 & \alpha_{13} & \alpha_{17} & \alpha_6 & \alpha_{19} & \alpha_{22} & \alpha_2 & \alpha_{20} & \alpha_9 & \alpha_{10} & \alpha_1 & \alpha_{12} & \alpha_7 & \alpha_{16} & \alpha_{11} & \alpha_{23} & \alpha_{21} & \alpha_{18} & \alpha_{15} & \alpha_{24} & \alpha_8 \\
\alpha_{15} & \alpha_7 & \alpha_9 & \alpha_{21} & \alpha_{19} & \alpha_{20} & \alpha_2 & \alpha_{12} & \alpha_3 & \alpha_{24} & \alpha_{14} & \alpha_8 & \alpha_{17} & \alpha_{11} & \alpha_1 & \alpha_{18} & \alpha_{13} & \alpha_{16} & \alpha_5 & \alpha_6 & \alpha_4 & \alpha_{23} & \alpha_{22} & \alpha_{10} \\
\alpha_{19} & \alpha_{21} & \alpha_{24} & \alpha_7 & \alpha_{15} & \alpha_3 & \alpha_{23} & \alpha_{14} & \alpha_{20} & \alpha_9 & \alpha_{12} & \alpha_{13} & \alpha_{11} & \alpha_{17} & \alpha_{18} & \alpha_1 & \alpha_8 & \alpha_5 & \alpha_{16} & \alpha_{10} & \alpha_{22} & \alpha_2 & \alpha_4 & \alpha_6 \\
\alpha_7 & \alpha_{15} & \alpha_{17} & \alpha_{24} & \alpha_{11} & \alpha_8 & \alpha_3 & \alpha_{16} & \alpha_2 & \alpha_{21} & \alpha_{10} & \alpha_{20} & \alpha_9 & \alpha_{19} & \alpha_{13} & \alpha_{23} & \alpha_1 & \alpha_{12} & \alpha_4 & \alpha_{22} & \alpha_5 & \alpha_{18} & \alpha_6 & \alpha_{14} \\
\alpha_{18} & \alpha_{23} & \alpha_{20} & \alpha_{22} & \alpha_{16} & \alpha_{10} & \alpha_{21} & \alpha_{13} & \alpha_{24} & \alpha_6 & \alpha_{17} & \alpha_{14} & \alpha_8 & \alpha_{12} & \alpha_{19} & \alpha_5 & \alpha_{11} & \alpha_1 & \alpha_{15} & \alpha_3 & \alpha_7 & \alpha_4 & \alpha_2 & \alpha_9 \\
\alpha_{16} & \alpha_{22} & \alpha_6 & \alpha_{23} & \alpha_{18} & \alpha_{24} & \alpha_4 & \alpha_{17} & \alpha_{10} & \alpha_{20} & \alpha_{13} & \alpha_{11} & \alpha_{12} & \alpha_8 & \alpha_5 & \alpha_{19} & \alpha_{14} & \alpha_{15} & \alpha_1 & \alpha_9 & \alpha_2 & \alpha_{21} & \alpha_7 & \alpha_3 \\
\alpha_{20} & \alpha_8 & \alpha_{18} & \alpha_{12} & \alpha_6 & \alpha_5 & \alpha_{11} & \alpha_2 & \alpha_{19} & \alpha_{16} & \alpha_7 & \alpha_4 & \alpha_{23} & \alpha_{22} & \alpha_{24} & \alpha_{10} & \alpha_{21} & \alpha_3 & \alpha_9 & \alpha_1 & \alpha_{17} & \alpha_{14} & \alpha_{13} & \alpha_{15} \\
\alpha_{22} & \alpha_{16} & \alpha_{12} & \alpha_{20} & \alpha_8 & \alpha_{11} & \alpha_{10} & \alpha_{15} & \alpha_4 & \alpha_{23} & \alpha_3 & \alpha_{24} & \alpha_6 & \alpha_{18} & \alpha_{14} & \alpha_{21} & \alpha_5 & \alpha_{17} & \alpha_2 & \alpha_7 & \alpha_1 & \alpha_{19} & \alpha_9 & \alpha_{13} \\
\alpha_{21} & \alpha_{19} & \alpha_{11} & \alpha_9 & \alpha_{17} & \alpha_{13} & \alpha_{20} & \alpha_5 & \alpha_{23} & \alpha_7 & \alpha_6 & \alpha_3 & \alpha_{24} & \alpha_{15} & \alpha_8 & \alpha_2 & \alpha_{18} & \alpha_{14} & \alpha_{22} & \alpha_4 & \alpha_{16} & \alpha_1 & \alpha_{10} & \alpha_{12} \\
\alpha_8 & \alpha_{20} & \alpha_{23} & \alpha_{16} & \alpha_{22} & \alpha_4 & \alpha_{19} & \alpha_3 & \alpha_{11} & \alpha_{12} & \alpha_{15} & \alpha_5 & \alpha_{18} & \alpha_6 & \alpha_{21} & \alpha_{14} & \alpha_{24} & \alpha_2 & \alpha_{17} & \alpha_{13} & \alpha_9 & \alpha_{10} & \alpha_1 & \alpha_7 \\
\alpha_6 & \alpha_{12} & \alpha_{16} & \alpha_8 & \alpha_{20} & \alpha_{19} & \alpha_{14} & \alpha_7 & \alpha_5 & \alpha_{18} & \alpha_2 & \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{10} & \alpha_{24} & \alpha_4 & \alpha_9 & \alpha_3 & \alpha_{15} & \alpha_{13} & \alpha_{11} & \alpha_{17} & \alpha_1
\end{pmatrix}$$

and $\sigma(v) = \sigma(v)^T$ if and only if $a_4 = a_{14}$, $a_6 = a_{24}$, $a_7 = a_{17}$, $a_8 = a_{23}$, $a_{11} = a_{12}$, $a_{16} = a_{19}$ and $a_{21} = a_{22}$. Next, consider elements of $\mathbb{F}_2((C_6 \times C_2) \rtimes C_2)$ of the form

$$\{\sum_{i=1}^{4}(\alpha_i y^{i-1} + \alpha_{i+4} x y^{i-1}) + \sum_{i=1}^{2}(\alpha_{i+8} x^2 y^{i-1} + \alpha_{i+12} y^{i+1} z) + (\alpha_{11} x^2 y^2 + \alpha_{17} x^2 z)(1+y)$$
$$+ \alpha_4 yz + \alpha_6 x^2 y^3 z + \alpha_7 xz + x^2 y^2 z \alpha_8 + \alpha_{12} z + \alpha_{14} x y^2 z + \alpha_{15} xyz + \alpha_{16} x y^3 z\}$$

and in particular the element $v_1 = 1 + [a + b + b^3 + (a + a^2)(b^2 + b^3)]c$ of this set. The matrix $\sigma(v_1)$ is equivalent to

$$\begin{pmatrix} I & A \end{pmatrix}$$

where

$$A = \begin{pmatrix}
0&1&0&1&1&0&1&1&0&0&1&1 \\
0&1&0&0&1&1&1&0&1&1&1&0 \\
1&0&1&0&1&0&1&1&1&0&1&0 \\
0&0&1&1&1&1&1&0&1&0&0&1 \\
1&1&0&1&1&1&0&0&0&1&0&1 \\
1&1&1&0&0&1&1&0&0&0&1&1 \\
1&1&0&0&0&0&0&1&1&1&1&1 \\
1&0&1&1&0&1&0&0&0&1&1&1&0 \\
1&1&0&1&0&1&1&1&1&0&0&0 \\
0&0&1&0&1&1&0&1&0&1&1&1 \\
1&0&1&1&0&0&1&1&0&1&0&1 \\
0&1&1&1&1&0&0&1&1&1&0&0
\end{pmatrix}.$$

It is a small computation to see that $C(v_1)$ is the $[24, 12, 8]$ code. Moreover, it can be shown that the above set contains 576 elements that generate the $[24, 12, 8]$ code.

3.4 The Group $SL(2, 3)$

Next we consider the group $SL(2, 3)$. Let v be the element

$$v = \sum_{i=1}^{6} x^{i-1} \left(\alpha_i + \alpha_{6+i} y + \alpha_{12+i} y^2 + \alpha_{18+i} y^2 x\right) \in \mathbb{F}_2 SL(2, 3)$$

where $SL(2,3) = \langle x, y \,|\, x^3 = y^3 = (xy)^2 \rangle$ and $\alpha_i \in \mathbb{F}_2$. Now,

$$\sigma(v) = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ A_5 & A_6 & A_7 & A_8 \\ A_9 & A_{10} & A_{11} & A_{12} \\ A_{13} & A_{14} & A_{15} & A_{16} \end{pmatrix},$$

where $A_1 = circ(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6)$, $A_2 = circ(\alpha_7, \alpha_8, \alpha_9, \alpha_{10}, \alpha_{11}, \alpha_{12})$,
$A_3 = circ(\alpha_{13}, \alpha_{14}, \alpha_{15}, \alpha_{16}, \alpha_{17}, \alpha_{18})$, $A_4 = circ(\alpha_{19}, \alpha_{20}, \alpha_{21}, \alpha_{22}, \alpha_{23}, \alpha_{24})$,
$A_5 = circ(\alpha_{16}, \alpha_{22}, \alpha_8, \alpha_{13}, \alpha_{19}, \alpha_{11})$, $A_6 = circ(\alpha_1, \alpha_{21}, \alpha_{14}, \alpha_4, \alpha_{24}, \alpha_{17})$,
$A_7 = circ(\alpha_7, \alpha_{20}, \alpha_5, \alpha_{10}, \alpha_{23}, \alpha_2)$, $A_8 = circ(\alpha_{18}, \alpha_{12}, \alpha_6, \alpha_{15}, \alpha_9, \alpha_3)$,
$A_9 = circ(\alpha_{10}, \alpha_{15}, \alpha_{21}, \alpha_7, \alpha_{18}, \alpha_{24})$, $A_{10} = circ(\alpha_{16}, \alpha_6, \alpha_{20}, \alpha_{13}, \alpha_3, \alpha_{23})$,
$A_{11} = circ(\alpha_1, \alpha_{12}, \alpha_{19}, \alpha_4, \alpha_9, \alpha_{22})$, $A_{12} = circ(\alpha_2, \alpha_{17}, \alpha_{11}, \alpha_5, \alpha_{14}, \alpha_8)$,
$A_{13} = circ(\alpha_9, \alpha_{14}, \alpha_{20}, \alpha_{12}, \alpha_{17}, \alpha_{23})$, $A_{14} = circ(\alpha_{15}, \alpha_5, \alpha_{19}, \alpha_{18}, \alpha_2, \alpha_{22})$,
$A_{15} = circ(\alpha_6, \alpha_{11}, \alpha_{24}, \alpha_3, \alpha_8, \alpha_{21})$, $A_{16} = circ(\alpha_1, \alpha_{16}, \alpha_{10}, \alpha_4, \alpha_{13}, \alpha_7)$.

Now, $\sigma(v) = \sigma(v)^T$ if and only if $\alpha_2 = \alpha_6$, $\alpha_3 = \alpha_5$, $\alpha_7 = \alpha_{16}$, $\alpha_8 = \alpha_{11}$, $\alpha_9 = \alpha_{19}$, $\alpha_{10} = \alpha_{13}$, $\alpha_{12} = \alpha_{22}$, $\alpha_{14} = \alpha_{24}$, $\alpha_{15} = \alpha_{18}$, $\alpha_{17} = \alpha_{21}$ and $\alpha_{20} = \alpha_{23}$. Next, consider elements of $\mathbb{F}_2 SL(2,3)$ of the form:

$$\begin{aligned}\{&\alpha_1 + \alpha_2(x + x^5) + \alpha_3(x^2 + x^4) + \alpha_4 x^3 + \alpha_5(y + x^3y^2) + \alpha_6(xy + x^4y) + \alpha_7(x^2y + y^2x) \\ &+ \alpha_8(x^3y + y^2) + \alpha_9(x^5y + x^3y^2x) + \alpha_{10}(xy^2 + x^5y^2x) + \alpha_{11}(x^2y^2 + x^5y^2) \\ &+ \alpha_{12}(x^4y^2 + x^2y^2x) + \alpha_{13}(xy^2x + x^4y^2x) \,|\, \alpha_i \in \mathbb{F}_2\}.\end{aligned}$$

It can be shown that it is not possible to construct the $[24, 12, 8]$ from any element of this set.

3.5 The Group $C_2^2 \times D_6$

Next we consider the group $C_2^2 \times D_6$. Let v be the element

$$v = \sum_{i=0}^{2} [(\alpha_{i+1} + \alpha_{i+4}z + \alpha_{i+7}w + \alpha_{i+10}zw) + b(\alpha_{i+13} + \alpha_{i+16}z + \alpha_{i+19}w + \alpha_{i+22}zw)]a^i \in \mathbb{F}_2(C_2^2 \times D_6)$$

where $\langle z, w \rangle = C_2^2$, $\langle a, b \rangle = D_6$ and $\alpha_i \in \mathbb{F}_2$. Now

$$\sigma(v) = \begin{pmatrix} A & B \\ B & A \end{pmatrix}$$

where $A = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ A_2 & A_1 & A_4 & A_3 \\ A_3 & A_4 & A_1 & A_2 \\ A_4 & A_3 & A_2 & A_1 \end{pmatrix}$, $B = \begin{pmatrix} B_1 & B_2 & B_3 & B_4 \\ B_2 & B_1 & B_4 & B_3 \\ B_3 & B_4 & B_1 & B_2 \\ B_4 & B_3 & B_2 & B_1 \end{pmatrix}$, $A_1 = cir(\alpha_1, \alpha_2, \alpha_3)$, $A_2 = cir(\alpha_4, \alpha_5, \alpha_6)$, $A_3 = cir(\alpha_7, \alpha_8, \alpha_9)$, $A_4 = cir(\alpha_{10}, \alpha_{11}, \alpha_{12})$, $B_1 = rcir(\alpha_{13}, \alpha_{14}, \alpha_{15})$, $B_2 = rcir(\alpha_{16}, \alpha_{17}, \alpha_{18})$, $B_3 = rcir(\alpha_{19}, \alpha_{20}, \alpha_{21})$ and $B_4 = rcir(\alpha_{22}, \alpha_{23}, \alpha_{24})$.
Now, $\sigma(v) = \sigma(v)^T$ if and only if $\alpha_2 = \alpha_3$, $\alpha_5 = \alpha_6$, $\alpha_8 = \alpha_9$ and $\alpha_{11} = \alpha_{12}$. Next, consider elements of $\mathbb{F}_2(C_2^2 \times D_6)$ of the form

$$\{\alpha_1 + \alpha_3 z + \alpha_5 w + \alpha_7 zw + (a + a^2)(\alpha_2 + \alpha_4 z + \alpha_6 w + \alpha_8 zw) + \sum_{i=0}^{2} + ba^i(\alpha_{i+13} + \alpha_{i+16} z + \alpha_{i+19} w + \alpha_{i+22} zw)\}.$$

It can be shown that it is not possible to construct the $[24, 12, 8]$ Golay code from any element of this set.

We summarize these results in the following: The $[24, 12, 8]$ Type II code can be constructed in $\mathbb{F}_2 G$ precisely for the following groups of order 24: S_4, D_{24}, $C_3 \times D_8$, $C_2 \times A_4$ and $(C_6 \times C_2) \rtimes C_2$.

4 The Dihedral Group

In this section, we shall describe these techniques for generating codes for the dihedral group. Let D_{2k} be the dihedral group of order $2k$. We describe the group by $D_{2k} = \langle a, b \mid a^2 = b^k = 1, ab = b^{-1}a \rangle$. The ordering of the elements for the map σ is $1, b, b^2, \ldots, b^{k-1}, a, ab, ab^2, \ldots, ab^{k-1}$. It is this group that McLoughlin used in [18] to give a construction of the binary $[48, 24, 12]$ extremal Type II code.

Let $v = \sum \alpha_{a^i, b^j} a^i b^j$. In this case, the matrix $\sigma(v)$ is of the form:

$$\begin{pmatrix} \alpha_1 & \alpha_b & \alpha_{b^2} & \ldots & \alpha_{b^{k-1}} & \alpha_a & \alpha_{ab} & \alpha_{ab^2} & \ldots & \alpha_{ab^{k-1}} \\ \alpha_{b^{k-1}} & \alpha_1 & \alpha_b & \ldots & \alpha_{b^{k-2}} & \alpha_{ab} & \alpha_{ab^2} & \alpha_{ab^3} & \ldots & \alpha_a \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_b & \alpha_{b^2} & \alpha_{b^3} & \ldots & \alpha_1 & \alpha_{ab^{k-1}} & \alpha_a & \alpha_{ab} & \ldots & \alpha_{ab^{k-2}} \\ \alpha_a & \alpha_{ab} & \alpha_{ab^2} & \ldots & \alpha_{ab^{k-1}} & \alpha_1 & \alpha_b & \alpha_{b^2} & \ldots & \alpha_{b^{k-1}} \\ \alpha_{ab} & \alpha_{ab^2} & \alpha_{ab^3} & \ldots & \alpha_a & \alpha_{b^{k-1}} & \alpha_1 & \alpha_b & \ldots & \alpha_{b^{k-2}} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{ab^{k-1}} & \alpha_a & \alpha_{ab} & \ldots & \alpha_{ab^{k-2}} & \alpha_b & \alpha_{b^2} & \alpha_{b^3} & \ldots & \alpha_1 \end{pmatrix}. \tag{11}$$

This gives that $\sigma(v)$ is of the form:

$$\begin{pmatrix} A & B \\ B & A \end{pmatrix}$$

where A is a circulant matrix and B is a reverse circulant matrix.

We begin by proving a lemma.

Lemma 4.1. *Let R be a finite commutative Frobenius ring of characteristic 2. Let C be the code generated by a matrix M of the form*

$$\begin{pmatrix} I_k & B \\ B & I_k \end{pmatrix},$$

where B is a symmetric k by k matrix. If the free rank of C is k then C is self-dual.

Proof. Let $D = \langle (I_k|B) \rangle$ and $D' = \langle (B|I_k) \rangle$. The inner-product of the i-th row of $(I_k|B)$ and the j-th row of $(B|I_k)$ is $B_{i,j} + B_{j,i} = 0$ since $B_{i,j} = B_{j,i}$ and the characteristic is 2. Therefore $D' = D^\perp$ since $|D||D'| = |R|^n$.

The code $C = \langle D, D^\perp \rangle$. If $D \neq D^\perp$ then $|C| > |D|$. However, we are assuming that the free rank of C is k. Hence $C = D = D^\perp$. This gives that C is a self-dual code. □

In [13], Hurley proves that C_v is self-dual over $\mathbb{F}_2$ if $v \in \mathbb{F}_2 D_{24}$, $v^2 = 0$ and the dimension is $\frac{n}{2}$. We can expand this by showing the following which eliminates the need for v to satisfy $v^2 = 0$.

Theorem 4.2. *Let R be a finite commutative Frobenius ring of characteristic 2 and let $v \in RD_n$ with $v = \sum \alpha_i h_i$ where only one $\alpha_{a^0 b^i}$ is 1 and the rest are 0. If C_v has free rank k, then C_v is a self-dual code.*

Proof. Since only one α_{2i} is 1 and the rest are 0, the generator matrix of C_v is permutation equivalent to a matrix of the form:

$$\begin{pmatrix} I_k & B \\ B & I_k \end{pmatrix}$$

where B is a reverse circulant matrix and hence symmetric. Then, by Lemma 4.1, we have the result. □

To show the importance of the strengthening of this result, consider the element $v = 1 + ab \in \mathbb{F}_2 D_{2k}$ where k is greater than 2. Then $(1e_{D_{2k}} + ab)^2 \neq 0$ but C_v is a self-dual code. We continue with a larger example.

Example 7. *Consider $v \in \mathbb{F}_2 D_{48}$ such that $dim(C_v) = 24$ and the minimum distance of C_v is 10. There are 192 elements v which produce equivalent self-dual codes using the technique. For more information about the importance of this result, see [8].*

A common technique for producing self-dual codes is to generate a code with the matrix $(I_{\frac{n}{2}}|A)$ where A is a reverse circulant matrix. Given a code C generated by this matrix we have that $C^\perp$ is generated by $(A^T|I_{\frac{n}{2}})$ which is equal to $(A|I_{\frac{n}{2}})$ since A is symmetric.

If C is a self-dual code then $\langle (A|I_{\frac{n}{2}})\rangle \subseteq \langle (I_{\frac{n}{2}}|A)\rangle$. This means that the code generated by $\begin{pmatrix} I_{\frac{n}{2}} & A \\ A & I_{\frac{n}{2}} \end{pmatrix}$ is the code C. Consider the first row of this matrix. Reading this as an element $v \in \mathbb{F}_2 D_{2k}$ we have that $C = C(v)$. This gives the following.

Theorem 4.3. *Let C be a binary self-dual code generated by $(I_{\frac{n}{2}}|A)$ where A is a reverse circulant matrix then $C = C(v)$ for some $v \in \mathbb{F}_2 D_{2k}$.*

Applying Corollary 2.3, we have the following.

Corollary 4.4. *The putative $[72, 36, 16]$ Type II code cannot be produced by $(I_{\frac{n}{2}}|A)$ where A is a reverse circulant matrix.*

Proof. Corollary 2.3 gives that the $[72, 36, 16]$ Type II code is not formed from an element in a group algebra and so Theorem 4.3 gives the result. □

This corollary eliminates a commonly used technique in the attempt to construct this putative code. Namely, many computational approaches to this problem have been to construct a reverse circulant matrix A and generate the code $(I_{\frac{n}{2}}|A)$. Of course, this technique has not yet produced the code. This corollary give a reason why these attempts have not been successful.

5 The Cyclic Group Cross the Dihedral Group

In this section, we shall use the group $G = C_s \times D_{2k}$. Let $C_s = \langle h \rangle$ and let $D_{2k} = \langle a, b \mid a^2 = b^k = 1, ab = b^{-1}a \rangle$. We shall order the elements as follows:

$$\{(1,1),(1,b),\ldots,(1,b^{k-1}),(h,1),(h,b),\ldots,(h,b^{k-1}),\ldots,(h^{s-1},1),$$
$$(h^{s-1},b),\ldots,(h^{s-1},b^{k-1}),(1,ab),\ldots,(1,ab^{k-1}),(h,1),(h,ab),\ldots,(h,ab^{k-1}),$$
$$\ldots,(h^{s-1},1),(h^{s-1},ab),\ldots,(h^{s-1},ab^{k-1})\}.$$

We see that if we choose $v \in RG$ such that only 1 of $\alpha_{(h^i,a^0b^j)}$ is 1 and the rest are 0. Then we get a matrix $\sigma(v)$ of the form:

$$\begin{pmatrix} I_k & B \\ B & I_k \end{pmatrix},$$

where B is of the following form:

$$B = \begin{pmatrix} 1A & hA & h^2A & \ldots & h^{s-1}A \\ h^{s-1}A & 1A & hA & \ldots & h^{s-2}A \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ hA & h^2A & h^3A & \ldots & 1A \end{pmatrix}$$

where $h^k A$ indicates the matrix where the i,j-th element is $(h^k, A_{i,j})$ and A is a reverse circulant matrix.

Theorem 5.1. *Let R be a Frobenius ring and let $v \in RC_sD_{2k}$ with $v = \sum \alpha_i h_i$ where only 1 of $\alpha_{(h^i,)a^0b^j}$ is 1 and the rest are 0. Let R be a finite commutative Frobenius ring of characteristic 2. If $|C_v| = |R|^{\frac{n}{2}}$, then C_v is isodual and hence formally self-dual with respect to any weight enumerator.*

Proof. We have that the code $C(v)$ is generated by $(I_k|B)$ and then its orthogonal is generated by $(B^T|I_k)$. Then we have that B is equivalent to B^T. Therefore $C(v)$ and $C(v)^\perp$ are equivalent and therefore, by Lemma 1.1, formally self-dual with respect to any weight enumerator. □

Note that if R is a finite field, then the condition in the previous theorem becomes that $dim(C_v) = \frac{n}{2}$.

Example 8. *Let G be the group C_3D_8. There are exactly $2^{12} = 4096$ elements in $\mathbb{F}_2G$ with the property that $\alpha_{(h^i,a^0b^j)}$ is equal to 1 when $i = j = 0$ and equal to 0 otherwise. Of these 256 have $dim(C_v) = 12$ and 192 of these codes are formally self-dual but not self-dual and 64 are self-dual. Of the 192 formally self-dual codes, 80 have minimum distance 6 which is optimal for Type I codes. As an example, if $v_1 = 1 + a(b + b(1 + b)(bh + h^2))$ then C_{v_1} is a formally self-dual code with minimum distance 6. The remaining 112 formally self-dual codes have have minimum distance 4 and C_{v_2} is an example of such a code where $v_2 = 1 + a(b^2 + h + b^3h + h^2 + bh^2)$.*

Example 9. *Let G be the group C_4D_8 and consider elements of $\mathbb{F}_2G$ with the property that $\alpha_{(h^i,a^0b^j)}$ is equal to 1 when $i = j = 0$ and equal to 0 otherwise. Of these elements, there are 2048 that have $dim(C_v) = 16$, of these 512 are self-dual and the remaining 1536 are formally self-dual. Let $v_1 = 1 + a(\hat{b} + h)h$, $v_2 = 1 + a(b + b^3 + h + h^3 + (b^2 + \hat{b})h^2 + (1 + \hat{b})h^3)$ and $v_3 = 1 + a(b(1 + h) + \hat{b}h^2 + (b + \hat{b})h^3)$. The code C_{v_1} is an example of a formally self-dual with minimum distance 4, the code C_{v_2} is an example of a formally self-dual with minimum distance 6 and the code C_{v_3} is an example of a formally self-dual with minimum distance 8. Of the 1536 formally self-dual codes, there are 896 with minimum distance 4, 192 with minimum distance 6 and 448 with minimum distance 8.*

Example 10. *Let G be C_5D_8 and $v = 1 + a((u + ub + ub^2 + b^3) + (u + b + b^2 + ub^3)(h + h^4) + (1 + b + ub^3)(h^2 + h^3)) \in R_1C_5D_8$. Then $C_v = \langle \sigma(v), u\sigma(v) \rangle$ is a self-dual code and its image under ϕ_1 is a binary self-dual $[80, 40, 12]$ code with an automorphism group of order 160.*

Example 11. *Let G be the group C_2D_{26} and consider the elements $\mathbb{F}_2$ with the properties that $\alpha_{(h^i,a^0b^j)}$ is equal to 1 when $i = j = 0$ and equal to 0 otherwise. Of these elements, there are six inequivalent self-dual $[52, 26, 10]$ codes. These six elements are as follows:*

i	$v_i \in \mathbb{F}_2(C_2D_{26})$	$\lvert Aut(C_{v_i})\rvert$
1	$1+a((b^8+b^{10}+b^{11}+b^{12})+(b+b^2+b^3+b^4+b^5+b^6+b^8+b^9+b^{11})h)$	52
2	$1+a((b^7+b^9+b^{10}+b^{11})+(1+b+b^2+b^3+b^5+b^7+b^8+b^{10}+b^{11})h)$	52
3	$1+a((b^6+b^8+b^{10}+b^{11}+b^{12})+(1+b+b^2+b^3+b^5+b^7+b^8+b^{11})h)$	52
4	$1+a((b^6+b^8+b^9+b^{10}+b^{11}+b^{12})+(1+b^2+b^3+b^4+b^6+b^7+b^8)h)$	52
5	$1+a((b^5+b^8+b^9+b^{10}+b^{12})+(b+b^3+b^4+b^6+b^7+b^9+b^{10}+b^{11})h)$	52
6	$1+a((b^5+b^7+b^8+b^9+b^{10}+b^{11}+b^{12})+(1+b+b^2+b^3+b^7+b^{11})h)$	52

6 The Cyclic Case

In this section, we shall set $G = C_n$ the cyclic group of order n. Since the inception of cyclic codes, it has been an open question to determine which cyclic codes were self-dual. We shall describe when this occurs.

We focus on the case when $n = 2k$. Let $G = \langle h \rangle$. Then let $h_i = h^i$. We then use as the ordering of the elements of G:

$$(h_0, h_2, \ldots, h_{2k}, h_1, h_3, \ldots, h_{2k-1}).$$

That is $g_i = h_{2(i-1)}$ for $i = 1$ to k and $g_{k+j} = h_{2(j-1)+1}$ for $j = 1$ to k.

It follows that the form of $\sigma(v)$ is:

$$\begin{pmatrix}
\alpha_{h_0} & \alpha_{h_2} & \cdots & \alpha_{h_{2k}} & \alpha_{h_1} & \alpha_{h_3} & \cdots & \alpha_{h_{2k-1}} \\
\alpha_{h_{2k}} & \alpha_{h_0} & \cdots & \alpha_{h_{2k-2}} & \alpha_{h_{2k-1}} & \alpha_{h_1} & \cdots & \alpha_{h_{2k-3}} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
\alpha_{h_4} & \alpha_{h_6} & \cdots & \alpha_{h_2} & \alpha_{h_3} & \alpha_{h_5} & \cdots & \alpha_{h_1} \\
\alpha_{h_{2k-1}} & \alpha_{h_1} & \cdots & \alpha_{h_{2k-3}} & \alpha_{h_0} & \alpha_{h_2} & \cdots & \alpha_{h_{2k}} \\
\alpha_{h_{2k-3}} & \alpha_{h_{2k-1}} & \cdots & \alpha_{h_{2k-5}} & \alpha_{h_{2k}} & \alpha_{h_0} & \cdots & \alpha_{h_{2k-2}} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
\alpha_{h_1} & \alpha_{h_3} & \cdots & \alpha_{h_{2k-1}} & \alpha_{h_4} & \alpha_{h_6} & \cdots & \alpha_{h_2}
\end{pmatrix}.$$

Hence $\sigma(v)$ is of the form

$$\begin{pmatrix} A & B \\ D & A \end{pmatrix}$$

where A, B and D are circulant matrices.

Choose an element of v such that $v = \sum \alpha_i h_i$ where only one of $\alpha_{2i} = 1$ and the rest of α_{2i} are 0. Then the generating matrix is permutation equivalent to a matrix where A is I_k and B and D are circulant matrices. Namely, we get a matrix of the form

$$\begin{pmatrix} I_{\frac{n}{2}} & B \\ D & I_{\frac{n}{2}} \end{pmatrix}.$$

Theorem 6.1. *Let R be a Frobenius ring of characteristic 2 and let $v \in RC_n$ with $v = \sum \alpha_i h_i$ where only one $\alpha_{2i} = 1$ and the rest of α_{2i} are 0. If $v_{2k-i} = v_i$ for odd i and $|C| = |R|^k$ then $C(v)$ is a self-dual code.*

Proof. By the construction, we have that $\sigma(v)$ is of the form

$$\begin{pmatrix} I_k & B \\ D & I_k \end{pmatrix}.$$

If $v_{2k-i} = v_i$ for odd i then $D = B^T$. We have that $|C| = |R|^k$. However, the form of the matrix gives that C contains a free code isomorphic to R^k, namely the code generated by the matrix $(I_k|B)$. This means that $C = \langle (I_k|B) \rangle$.

Consider the code generated by the matrix $(B^T|I_k)$. This code must be $C^\perp$. However, this code is contained in $C(v)$ as well, so we have that $C = C^\perp$. □

Notice that we did not have to determine the cardinality of the code to see that the code was self-dual.

Note that it is certainly more difficult to use this technique to construct self-dual codes with the cyclic group. That is, we had to put more restrictions on v to obtain a self-dual code. This is certainly to be expected since it is fairly difficult to find cyclic self-dual codes.

Moreover, note that a code over R_k constructed with this technique is cyclic, which gives that its image under the Gray map is quasi-cyclic of index 2^k.

Example 12. *Let G be the cyclic group of order 10 and $v = 1+uh+h^5+uh^9 \in R_1C_{10}$. Then $C_v = \langle \sigma(v), u\sigma(v) \rangle$ is cyclic self-dual code and its image under ϕ_1 is a binary quasi-cyclic self-dual $[20, 10, 4]$ code of index 2.*

We note that this is a standard construction of self-dual codes, namely you take a vector $\mathbf{v}$ and generate a circulant matrix B from it with $BB^T = -I_k$, with $n = 2k$, and generate the code $(I_k|B)$. Hence, we have another of the standard constructions of self-dual codes within our general framework.

We can now use our general construction to produce isodual codes.

Theorem 6.2. *Let R be a finite commutative Frobenius ring with characteristic 2. Let $v \in RC_n$ with $v = \sum \alpha_i h_i$ where only one $\alpha_{2i} = 1$ and the rest of α_{2i} are 0. If $|C(v)| = |R|^{\frac{n}{2}}$ then $C(v)$ is a formally self-dual code with respect to any weight enumerator.*

Proof. If $|C(v)| = |R|^{\frac{n}{2}}$ then C is generated by the matrix $(I_k|B)$ where B is a circulant matrix. Then its orthogonal is of the form $(B^T|I_k)$. Since B is a circulant code, then by permuting the rows and columns of B we can form B^T. This gives that $C(v)^\perp$ is equivalent to $C(V)$ and hence isodual and therefore formally self-dual code with respect to any weight enumerator. □

Example 13. *Let G be the cyclic group of order 6 and $v = 1+u_2h+(1+u_1+u_1u_2)h^3+u_1h^5 \in R_2C_6$. Then $C_v = \langle \sigma(v), u_1\sigma(v), u_1u_2\sigma(v)\rangle$ is a cyclic formally self-dual code and its image under ϕ_2 is a binary quasi-cyclic self-dual $[24, 12, 6]$ code of index 4.*

Example 14. *Let G be the cyclic group of order 10. The following elements of R_2C_{10} generate four inequivalent binary self-dual $[40, 20, 8]$ codes:*

i	$v_i \in R_2C_{10}$	$\lvert Aut(C_{v_i})\rvert$
1	$1 + u_1(h + h^9) + u_2(h^3 + h^7) + h^5$	$2^{16} \cdot 3^3 \cdot 5^2$
2	$1 + u_1(h + h^9) + u_2(h^3 + h^7) + (u_1u_2 + 1)h^5$	$2^{14} \cdot 3 \cdot 5$
4	$1 + u_1(h + h^9) + u_2(h^3 + h^7) + (u_2 + 1)h^5$	$2^{14} \cdot 3 \cdot 5$
5	$1 + u_1(h + h^9) + u_2(h^3 + h^7) + (u_1 + u_1 + 1)h^5$	$2^{16} \cdot 3^3 \cdot 5^2$

7 Quasi-G Codes

In this section, we make a generalization of the notion of a quasi-cyclic group. In general, quasi-cyclic groups are more difficult to handle that cyclic codes because they do not have a canonical representation in an algebraic setting the way that cyclic codes do. In [6], a ring was developed with a Gray map that could be used to describe certain families of quasi-cyclic groups. That same ring can be used in this setting to construct quasi-G codes which we shall describe below. Self-dual codes over these rings were studied in [7].

Let G be a finite group of order n and R a finite Frobenius commutative ring. Let D be a code in R^{sn} where the coordinates can be partitioned into n sets of size s where each set is assigned an element of G. If the code D is held invariant by the action of multiplying the coordinate set marker by every element of G then the code D is called a quasi-group code of index s.

We now describe a family of rings to construct quasi-G codes.

Let $p_1, p_2, \ldots, p_t$ be prime numbers with $t \geq 0$ and $p_i \neq p_j$ if $i \neq j$. Define Δ to be $\Delta = p_1^{k_1}p_2^{k_2}\cdots p_t^{k_t}$, for some $k_i \geq 1$, $i = 1, \ldots, t$.

The ring is defined as follows:

$$R_{q,\Delta} = \mathbb{F}_q[u_{p_1,1}, \ldots, u_{p_1,k_1}, u_{p_2,1} \ldots, u_{p_2,k_2}, \ldots, u_{p_t,k_t}]/\langle u_{p_i,j}^{p_i} = 0\rangle,$$

where the indeterminates $\{u_{p_i,j}\}_{(1\leq i\leq t, 1\leq j\leq k_i)}$ commute.

Let $i \in \{1, \cdots, t\}$, $j \in \{1, \cdots, k_i\}$. Take the set of exponents $J_i = \{0, 1, \ldots, p_i - 1\}$ for the indeterminant $u_{p_i,j}$. For $\alpha_i \in J_i^{k_i}$ denote $u_{p_i,1}^{\alpha_i,1} \cdots u_{p_i,k_i}^{\alpha_i,k_i}$ by $u_i^{\alpha_i}$. For a monomial $u_1^{\alpha_1} \cdots u_t^{\alpha_t}$ in $R_{q,\Delta}$ write u^α, where $\alpha = (\alpha_1, \ldots, \alpha_t) \in J_1^{k_1} \times \cdots \times J_t^{k_t}$.

Let $J = J_1^{k_1} \times \cdots \times J_t^{k_t}$. Any element c in $R_{q,\Delta}$ can be written as

$$c = \sum_{\alpha\in J} c_\alpha u^\alpha = \sum_{\alpha\in J} c_\alpha u_{p_1,1}^{\alpha_1,1} \cdots u_{p_1,k_1}^{\alpha_1,k_1} \cdots u_{p_t,1}^{\alpha_t,1} \cdots u_{p_t,k_t}^{\alpha_t,k_t}, \tag{12}$$

with $c_\alpha \in \mathbb{F}_q$.

It is immediate that $R_{q,\Delta}$ is a commutative ring with $|R_{q,\Delta}| = q^{p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}} = q^\Delta$.

Next we define a Gray map on this ring. We will consider the elements in $R_{q,\Delta}$ as q-ary vectors of Δ coordinates. Order the elements of A_Δ lexicographically and use this ordering to label the coordinate positions of $\mathbb{F}_q^\Delta$. Define the Gray map $\Psi_\Delta : A_\Delta \to \mathbb{F}_q^\Delta$ as follows:

$$\Psi_\Delta(a)_b = \begin{cases} 1 & \text{if } \widehat{b} \subseteq \{\widehat{a} \cup 1\}, \\ 0 & \text{otherwise,} \end{cases}$$

where $\Psi_\Delta(a)_b$ indicates the coordinate of $\Psi_\Delta(a)$ corresponding to the position of the element $b \in A_\Delta$ with the defined ordering.

It follows that $\Psi_\Delta(a)_b$ is 1 if each indeterminate $u_{p_i,j}$ in the monomial b with non-zero exponent is also in the monomial a with the same exponent. In other words, it is 1 when $\widehat{b}$ is a subset of $\widehat{a}$. In order to consider all the subsets of $\widehat{a}$, we also add the empty subset that is given when $b = 1$; that is we compare $\widehat{b}$ to $\widehat{a} \cup 1$.

Finally, we extend Ψ_Δ linearly for all elements of $R_{q,\Delta}$. Then Ψ_Δ is a Gray map from $R_{q,\Delta}$ to $\mathbb{F}_q^\Delta$. Note that the ring R_k is $R_{2,2^k}$ in this setting.

Theorem 7.1. *Let C be a code in ${R_{q,\Delta}}^n$ for a finite group G, that is C is a G-code. Then $\Psi_\Delta(C)$ is a quasi-G code of length $n\Delta$ of index Δ in $\mathbb{F}_q^{\Delta n}$.*

Proof. Let $\mathbf{v} \in C$. If g is an element of the group G then g acts on the set of Δ coordinates corresponding to the element $v_i \in R_{q,\Delta}$, that is on $\Psi_\Delta(v_i)$ and sends them to the coordinates corresponding to $\Psi_\Delta(gv_i)$. Therefore, the image is a quasi-G group of index Δ. □

An identical proof gives the following.

Theorem 7.2. *Let C be a quasi-G code of length n and of index k over $R_{q,\Delta}$ for a finite group G, that is C is a G-code. Then $\Psi_\Delta(C)$ is a quasi-G code of length $n\Delta$ of index $k\Delta$ in $\mathbb{F}_q^{\Delta n}$.*

Example 15. *In Example 5, it is shown that if $v = u(b + ab + ac + bc^2) + (bc + bc^2) + (1 + u)(c^2 + abc^2) \in R_1A_4$, then, C_v is a self-dual code of length 12 over R_1. This gives that $\phi_1(C)$ is the length 24 binary Golay code. It follows then that the binary $[24, 12, 8]$ Golay code is a quasi-Alternating group of order 4 code with index 2.*

Example 16. *In Example 10, it is shown that if $v = 1 + a((u + ub + ub^2 + b^3) + (u + b + b^2 + ub^3)(h + h^4) + (1 + b + ub^3)(h^2 + h^3)) \in R_1C_5D_8$, then $C_v = \langle \sigma(v), u\sigma(v) \rangle$ is the binary $[80.40, 12]$ self-dual code under ϕ_1. Therefore this code is a quasi-C_5D_8 code of index 2.*

Example 17. *In Example 14, it is shown that inequivalent binary self-dual $[40, 20, 8]$ codes are constructed from R_2C_{10}. It follows that these four codes are quasi-cyclic code of index 4.*

8 Conclusion

In this paper, we have considered a very broad generalization of the notion of cyclic codes by examining codes that are ideals in a group ring, calling these codes G-codes. Similar theorems to the standard results on cyclic codes have been attained. For instance, we have shown that the dual of G-code is again a G-code. This natural algebraic setting allows for canonical constructions of families of codes and for ensuring that the automorphism group of a code contains a given group. We used the Chinese Remainder Theorem to construct G-codes over arbitrary rings from G-codes over local rings.

Based on some previously known constructions for group algebras, we have given generalized constructions of self-dual codes in this setting for codes over a Frobenius ring. We have given the form of the generator matrix for codes in this construction for various groups. We have shown precisely which groups will give the binary Golay self-dual code in this setting, namely the Golay code is a G-code for the following groups: S_4, D_{24}, $C_3 \times D_8$, $C_2 \times A_4$ and $(C_6 \times C_2) \rtimes C_2$.

The ring family of rings R_k has also been used to construct interesting binary self-dual codes via the canonical Gray map. This allows for a construction of longer self-dual and formally self-dual binary codes.

The notion of quasi-cyclic codes has also been generalized and we have used the family of rings $R_{q,\Delta}$ to produce families of quasi-G codes over a finite Frobenius ring. We have given several examples of binary quasi-G codes for various groups.

The fundamental open question is to determine which codes are G-codes for a finite group G. That is, given an arbitrary code over a ring R, for which groups G can C be seen as an ideal in RG. Since even the case when G is the cyclic group (cyclic codes) remains a large area of research, it seems that there is a great deal of work to be done in this area. More computationally, it should be determined which self-dual codes (especially optimal self-dual codes) can be constructed via the methods described in this paper. Within this framework, these computational techniques can be extended to numerous families of rings and numerous groups.

References

[1] Bernhardt, F., Landrock, P., Manz, O., The extended Golay codes considered as ideals, J. Combin. Theory Ser. A, **55**, no. 2., 1990, 235 - 246.

[2] Borello, M., The automorphism group of a self-dual $[72, 36, 16]$ code is not an elementary abelian group of order 8, Finite Fields Appl. **25**, 2014, 1 - 7.

[3] Bouyuklieva, S., On the automorphism of order 2 with fixed points for the extremal self-dual codes of length $24m$, *Des. Codes Cryptogr.*, **25**, no. 1, 2002, 5 - 13.

[4] Bouyuklieva, S., O'Brien, E.A. Willems, W., The automorphism group of a binary self-dual doubly-even $[72, 36, 16]$ code is solvable, *IEEE Trans. Inform. Theory*, **52**, 2006, 4244 - 4248.

[5] Dougherty, S.T., Algebraic Coding Theory Over Finite Commutative Rings, Springer-Verlag, Springer Briefs in Mathematics (ISBN 978-3-319-59805-5), 2017.

[6] Dougherty, S.T., Fernandez-Cordoba, D., Ten-Valls, R., Quasi-Cyclic Codes as Cyclic Codes over a Family of Local Rings, Finite Fields and Their Apps., **40**, 2016, 138 - 149.

[7] Dougherty, S.T., Kaya, A., Salutrk, E., Constructions of Self-Dual Codes and Formally Self-Dual Codes over Rings, AAECC, DOI 10.1007/s00s00-016-0288-5, 2016.

[8] Dougherty, S.T., Kim, J.L., Solé, P., Open Problems in Coding Theory, Contemporary Mathematics, **634**, 2015, 79 - 99.

[9] Dougherty, S.T., Yildiz, B., Karadeniz, S., Codes over R_k, Gray maps and their Binary Images, with Finite Fields and their Applications, **17**, no. 3, 2011, 205 - 219.

[10] Dougherty, S.T., Yildiz, B., Karadeniz, S., Cyclic Codes over R_k, Designs, Codes and Cryptography, **63**, no. 1., 2012, 113 - 126.

[11] Dougherty, S.T., Yildiz, B., Karadeniz, S., Self-dual codes over R_k and binary self-dual codes. Eur. J. Pure Appl. Math. **6**, no. 1, 2013, 89 - 106.

[12] The GAP Group, GAP – Groups, Algorithms and Programming, Version 4.4, 2006 (http:/www.gap-system.org).

[13] Hurley, T., Group Rings and Rings of Matrices, Int. Jour. Pure and Appl. Math,, **31**, no. 3, 2006, 319 - 335.

[14] Lam, C. W. H.; Thiel, L.; Swiercz, S. The nonexistence of finite projective planes of order 10. Canad. J. Math. **41**, no. 6, 1989, 1117 - 1123.

[15] MacWilliams, F. J., Binary codes which are ideals in the group algebra of an Abelian group. Bell System Tech. J. **49**, 1970, 987 - 1011.

[16] MacWilliams, F.J., Codes and ideals in group algebras. 1969 Combinatorial Mathematics and its Applications (Proc. Conf., Univ. North Carolina, Chapel Hill, N.C., 1967) 317 - 328. Univ. North Carolina Press, Chapel Hill, N.C.

[17] McLoughlin, I., Dihedral codes, Ph.D. thesis, National University of Ireland, Galway, 2009.

[18] McLoughlin, I., A group ring construction of the $[48, 24, 12]$ Type II linear block code, Des. Codes Cryptogr., **63**, no. 1, 2012, 29 - 41.

[19] McLoughlin, I., Hurley, T., A group ring construction of the extended binary Golay code, IEEE Trans. Inform. Theory, **54**, no. 9, 2008, 4381 - 4383.

[20] Nebe, G., An extremal $[72, 36, 16]$ binary code has no automorphism group containing $\mathbb{Z}_2 \times \mathbb{Z}_4, Q_8$ or $\mathbb{Z}_{10}$, *Finite Fields Appl.*, **18**, no. 3, 2012, 563 - 566.

[21] O'Brien, E.A., Willems, W., On the automorphism group of a binary self-dual doubly-even $[72, 36, 16]$ code, *IEEE Trans. Inform. Theory*, **57**, no.7, 2011, 4445 - 4451.

[22] Yankov, N., A putative doubly-even $[72, 36, 16]$ code does not have an automorphism of order 9, *IEEE Trans. Inform. Theory*, **58**, no. 1, 2012, 159 - 163.